INDIANA PROSECUTING ATTORNEYS COUNCIL

Presentation on

"INVESTIGATIONS"

Lecture by Richard J. Hertel

Ripley County Prosecuting Attorney

DISCUSSION NOTES AND OUTLINE

Subpoenas Duces Tecum

[IC 35-37-5-2; Ind.R.Cr.P. 2; In.R.Tr.P. 45, 4, 4.16, 5]

What is the purpose of a subpoena duces tecum?

A subpoena duces tecum is a court order to produce evidence (books, papers, documents, or tangible things designated by the subpoena).

How to subpoena:

Pre-charge subpoena procedure:
1. Motion the Court with jurisdiction over the matter, ex parte
2. Attach the subpoena with requested materials
3. Serve the subpoena

Post-Charge subpoena procedure:
1. Motion the Court
2. Maybe a hearing
3. Give notice to the Defense
4. Not ex parte

Service of subpoena

A sheriff, deputy, party, or "any person" may serve the subpoena by mail, personally, through an agent of the person served, or by leaving a copy at his dwelling or business. If someone besides a sheriff or deputy serves the subpoena, proof of service must be shown by affidavit. Without proof of proper service, the subpoena cannot be enforced. All parties must be served with a copy, and failure to obey the subpoena may be deemed contempt.

Source of Prosecutorial Subpoena Power

A prosecutor's investigatory power parallels that of a grand jury. *See In re Order for Indiana Bell Telephone to Disclose Records* 409 N.E.2d 1089 (Ind. 1980). However, a prosecutor acting without a grand jury must seek leave of court before issuing a subpoena duces tecum, and the subpoena must meet certain reasonableness standards (described in the next subsection). *Oman v. State*, 737 N.E.2d 1131, 1148 (Ind. 2000).

Oman limited the prosecutorial subpoena power by requiring leave of court to issue subpoenas. However, it is also significant in that it affirms the authority of a prosecutor to issue subpoenas so long as the requirements are met.

Additionally, IC 33-39-1-4 states that prosecutors who have received information about a crime shall cause process to issue from the court with jurisdiction over the crime, directing the proper officer to subpoena persons likely to have information about the crime (witnesses or persons possessing evidence). This means that prosecutors have a duty to investigate crimes using tools like subpoenas. This statute also states that the prosecutor shall examine persons subpoenaed; thus, prosecutors have a clear source of authority for prosecutorial subpoena power.

When to use a subpoena

A subpoena is a useful means of obtaining evidence when there is less than probable cause. The investigatory nature of subpoenas is why probable cause is not necessary. However, a prosecutor may not act arbitrarily or outside of statutory authority in issuing subpoenas, and must be reasonable (limited scope, relevant, and specific enough so as to not be unreasonably burdensome). *See State ex rel. Pollard v. Crim. Court of Marion County*, 329 N.E.2d 273 (Ind. 1975).

Quashing or modification of the subpoena

Subpoenas can be quashed on the basis of the privilege against self-incrimination (unless use immunity has been granted), or if compliance with the subpoena is unreasonable or oppressive. The decision of whether to quash, modify, or enforce the subpoena is a question for the Court to decide. *Turpin v. State*, 435 N.E.2d 573 (Ind. 1975).

See appendix for a sample subpoena duces tecum and Motion and Order for Subpoena Duces Tecum.

Subpoena ad Testificandum [In.R.Tr.P. 45; IC 35-37-5-2]

What is a subpoena ad testificandum?

This is a court order for a witness to give testimony. This type of subpoena may implicate the privilege against self-incrimination, while a subpoena duces tecum usually does not. Once the subpoena has been served, the witness may only be released by the issuing court. The prosecutor cannot release a witness under subpoena; doing so may result in serious consequences from the court.

When to use:

Like the subpoena duces tecum, the subpoena ad testificandum is an equally useful tool to gain a better understanding of a crime. It is equally useful for evidentiary purposes, depending on what kind of testimony is sought. This type of subpoena is just as useful as a subpoena duces tecum, and can be used in the same types of cases and situations.

How to use:

The procedure for issuing this kind of subpoena (often referred to as simply a "subpoena," as opposed to the subpoena duces tecum, which is frequently called by the full Latin name) is the same. Subpoenas ad testificandum are largely controlled by the same laws as subpoenas duces tecum. *See* IC 35-37-5-2; *Oman v. State*. However, Ind. R. Cr. P. 2 only addresses subpoenas duces tecum. TR 45 addresses subpoenas for the purpose of taking depositions; these would fall under the category of subpoena ad testificandum, as purpose is to obtain testimony, not tangible things. Thus, these subpoenas are not limited to appearances in court, but can also compel a witness to appear for discovery purposes.

Quashing or modification of the subpoena:

Newton v. Yates (353 N.E.2d 485 (Ind. Ct. App. 1976)) addressed the issue of quashing subpoenas ad testificandum, requiring immateriality, irrelevancy, and inadmissibility for quashing a subpoena. *In re Adoption of L. C.* 650 N.E.2d 726, 732 (Ind. Ct. App. 1995) developed this further, stating that quashing is improper where a witness potentially possesses some relevant and admissible evidence to offer at trial.

Uniform Act to Secure the Attendance of Witnesses from Outside the State in Criminal Proceedings [IC 35-37-5]

This act, applicable in all 50 states, D.C., Puerto Rico, and the Virgin Islands, provides procedure for obtaining the testimony of out-of-state witnesses. The court in which the trial is to be held may issue either a subpoena duces tecum or a subpoena ad testificandum, and the form and service requirements are the same as for an in-state witness. This act also provides for the transfer of an imprisoned or institutionalized witness.

To subpoena a witness under the act (pursuant to 35-37-5-2), the State or defendant must seek a subpoena from the county in which the desired witness resides. The subpoena must be issued by that county's clerk under seal, state the name of the court and title of the action, command the witness to attend and give testimony at a specified time and place, and be signed by the clerk. The judge may specify the number of days the witness is required to be present, and the witness shall not be required to stay longer than this period. 35-37-5-5 provides that fees may be paid to these witnesses and that

persons refusing to comply with a subpoena may be punished in the same manner as an in-state witness who similarly refuses.

The witness must be material, and the party seeking attendance of the out of state witness must satisfy the statutory procedural requirements. However, the Uniform Act is not the only way to obtain out of state witnesses; witnesses may also voluntarily respond to a request to cross state lines and testify. *Forbes v. State,* 810 N.E.2d 681, 684 (Ind. 2004).

Problems:

As mentioned above, this type of subpoena necessarily implicates the Fifth Amendment privilege against self-incrimination. *State ex rel. Pollard* (329 N.E.2d 573, 590 (Ind. 1975)) held that an accused who refuses to comply with either form of subpoena cannot be held in contempt (although other witnesses may be).

Where witnesses other than the accused invoke the privilege against self-incrimination, the prosecutor cannot petition the court for use immunity and compel the witness to testify without filing charges or convening a grand jury. *In re S.H.*, 984 S.E.2d 630, 636 (Ind. 2013). Thus, it can be very hard to get this kind of testimonial evidence through a subpoena after privilege is invoked.

See appendix for an example of a subpoena ad testificandum.

Search Warrants [IC 35-33-5-1 et seq.; IC 35-33.5-2-1; IN Const. Art. 1, § 11]

What is the purpose of a search warrant?

A warrant is a tool to obtain evidence. The use of a warrant assists in the protection of evidence against allegations of wrongdoing, reducing the risk of exclusion. The main purpose of a search warrant is to prevent violations of individual rights. The Indiana Constitution and the 4th Amendment of the US Constitution contain the same prohibitions on unreasonable search and seizure and requirements of probable cause, oath or affirmation in support, and particularity.

How to Obtain a Warrant

A warrant must be supported by an affidavit and filed with the judge. The affidavit must contain sufficiently particular descriptions, substantial allegations of the offense and the affiant's belief and good cause to believe the things sought are concealed there, and the facts known by the affiant constituting probable cause. Where the facts constituting

probable cause contain hearsay, the affidavit must contain reliable information establishing credibility and factual basis or the totality of circumstances corroborating.

Warrant Execution

Under IC 35-33-5-7, a search warrant issued by a court of record may be executed by its terms anywhere in the state. If not issued by a court of record, it may be executed in the county in which it was issued. A search warrant may be executed any day of the week, at any time of day. The officers executing the warrant must knock prior to forcibly entering, absent exigent circumstances sufficient to justify the no-knock entry (for example, if the officer has reasonable suspicion that knocking and announcing would be dangerous based on past observations of the suspect regularly carrying a handgun and statements of the suspect from a confidential informant that the suspect would "take out as many cops as possible).

Practice Tips:

Although the search and seizure provision (Art. 1, § 11) of the Indiana Constitution uses the same language as the federal constitution, Indiana courts interpret and apply this provision independently from federal Fourth Amendment jurisprudence. What is reasonable under the federal constitution may not always be reasonable under §11. *Mitchell v. State*, 745 N.E.2d 775, 785 (Ind. 2001).

See appendix for affidavit and warrant forms.

SCHOOLS

What types of information could be obtained from a school?

Schools possess records of student attendance, disciplinary records, mental health records and grades. The type of case will dictate which type of record may be useful. Random drug tests of students could also be available (these tests were upheld in *Link v. Northwestern School Corp.*, 763 N.E.2d 972 (Ind. 2002)).

How to get this information

The best way to get this information is to ask the parents or guardians to sign a consensual release of the information. A search warrant would be equally useful, although it would require probable cause. A subpoena duces tecum could be used where there is less than probable cause.

Interagency Cooperative Agreement [IC 31-39-2-9]

Another option for gathering information from schools would be an information-sharing agreement between the school district, local law enforcement, DCS, the prosecutor's office, and the probation office. Pursuant to state law, information regarding juveniles may be shared between agencies where there is a signed agreement. Once the agreement is in force, information could be obtained with just a phone call to one of the agencies.

Procedure for obtaining the agreement:
1. Circuit Court Judge approval and issuance of order
2. Approval by all agencies and designation of information "gatekeepers"

For a sample information-sharing agreement, see the appendix

Problems:

FERPA (20 U.S.C. § 1232g(a)(1)(A)) protects educational records from disclosure without consent of the student or guardian, if the student is a minor. "Directory information" like names, addresses, honors, and awards is not protected under FERPA. As a prosecutor, FERPA should not bar access to records; consent is not required to disclose protected education records to a state or local authority within the juvenile justice system, or to comply with a lawful subpoena or court order.

HOSPITALS

What information?

Medical records, mental health records, and treatment information/ schedule

When to use:

Medical records are useful in a wide variety of cases, from mental health records, to blood draws for DUIs, to treatment records in domestic violence cases.

How to obtain:

The easiest way to obtain this information is through a consensual release (in a signed writing, patient asks health care provider to waive privacy and release the records). However, note that different hospitals could each require a different consent form, especially as between hospitals in different states. **See appendix for sample release agreement.**

Subpoenas and warrants are also possible options. As discussed below, medical records may be obtained through a subpoena or warrant without violating individual privacy rights. Subpoenas duces tecum and warrants for medical records are generally subject to the same standards and requirements as in other circumstances.

Although Indiana has a statutory physician-patient privilege (under IC 34-46-3-1, physicians shall not be required to testify as to matters communicated to them by patients), the privilege can be waived (for example, by the patient providing information on the privileged matters to police or putting the information at issue with a civil suit). The Indiana Supreme Court has held that the privilege is not absolute, and it is for the benefit of the patient in receiving health care; thus, a trial court may allow discovery of even non-party medical records with adequate safeguards to protect the confidentiality and identity of a patient. *Terra Haute Regional Hosp., Inc. v. Trueblood*, 600 N.E.2d 1358, 1362 (Ind. 1992). However, the discovery must be reasonable. For example, the State cannot seize all records from a practice to search for evidence of child molestation; the discovery must be reasonable in scope, since the State recognizes a legitimate privacy interest in medical records. *Planned Parenthood of Indiana v. Carter*, 854 N.E.2d 853, 884-8 (Ind. Ct. App. 2006).

HIPAA Issues

HIPPA (the Health Insurance Portability and Accountability Act of 1996; *see* 45 C.F.R. 160 and 164 for the Privacy Rule) protects individuals from dissemination of medical and mental health records without consent. Under HIPAA, health care providers cannot release individually identifiable health information except as the Privacy Rule permits or requires, or if the individual (the patient) authorizes in writing (a consensual release). Required releases are to the federal HHS, or to the patient directly. Permitted releases include one which is relevant to our discussion: "public interest and benefit activities." This category includes release as required by law (pursuant to law or court order), to appropriate government authorities for preventing disease, injury, child abuse, neglect, or domestic violence, and to law enforcement officials for law enforcement purposes.

The law enforcement exceptions are the most important for prosecuting crimes. There are six categories of enforcement exceptions, 5 of which are relevant for prosecution: 1. as required by law (court order/ subpoena/ warrant); 2. to identify or locate a suspect, fugitive, material witness, or missing person; 3. to alert law enforcement about a death where the health care provider suspects the death was caused by criminal activity; 4. where the provider believes the health information is evidence of a crime that occurred on its premises; and 5. when necessary to inform law enforcement about the commission, location, and nature of a crime, crime victim, or evidence. Other exceptions that could be useful are where the provider believes disclosure is necessary to prevent or lessen a

serious threat to health or safety (of either the patient or the public), and for essential government functions (e.g. if the patient is a prisoner).

Disclosure under HIPAA must be of the minimum information necessary unless the disclosure is pursuant to a release authorization, or where the disclosure is required by law. Finally, although state laws contrary to HIPAA are generally preempted, there are exceptions for compelling public health, safety, and welfare needs, although those needs must be balanced against the individual privacy interests and state laws regarding manufacture, registration, distribution, or other control of controlled substances.

Authorization for release of information under HIPAA must contain the following core elements: specific and meaningful description of the information to be disclosed, name or identification of the person making the disclosure and the person to whom it is made, the purpose of the disclosure, an expiration date or event to end the disclosure, and a signature and date from the individual. 45 C.F.R. § 164.508(c). The authorization must also have statements to put the patient on notice of the right to revoke authorization, whether treatment or benefits are conditioned on the authorization, and the potential for later redisclosure that could remove the protection of the information.

BANKS

What type of information?

Financial records, transaction records

When will this information be useful?

Bank records may be very useful in a variety of cases such as fraud, theft, deception, or robbery.

How to obtain?

Bank records are fairly easy to obtain by consent. A bank could provide an authorization for release of records under specific circumstances in the terms of agreement to open the account. Alternately, the State can subpoena bank records (so long as the subpoena meets the standards discussed above). There is no reasonable expectation of privacy in customer records, checks, and bank slips where the information is voluntarily conveyed to the bank and exposed to employees in the ordinary course of business (such that a subpoena for these limited types of banks records is not an unreasonable search and seizure). *In re Thompson*, 479 N.E.2d 1344, 1346 (Ind. Ct. App. 1985); *U.S. v. Miller*, 425 U.S. 435, 440 (1976).

Some cases have held that there is an implied duty not to disclose information about customers' financial statuses unless a public duty arises. *Indiana Nat. Bank v. Chapman*, 482 N.E.2d 474, 482 (Ind. Ct. App. 1985). Compliance with a valid court order, subpoena, or warrant in the course of a legitimate criminal investigation ("communication to legitimate law enforcement inquiry") is sufficient for public duty to overcome the implied duty not to disclose. *Id.* Although a warrant for these records could be used, a subpoena will generally be sufficient given the nature of the records.

SOCIAL MEDIA/ WEBSITES/ EMAIL

What information is available?

Social media accounts- personal identification, posts (statements and photographs). Websites- search history. Emails- contact lists, messages.

When is it useful?

This information may be useful in a wide variety of cases, from child pornography, to harassment, to drug trafficking and dealing. Electronic records can provide evidence of almost anything by proving admission of guilt, incriminating statements or even culpability itself.

How to obtain this information

Warrant:

A warrant is the best option, given the nature of this information (very personal, detailed, extensive, private information, and the fact that the increased procedural protection will help counter any later challenge to the search and seizure). Additionally, the law regarding social media accounts is still developing; as more social media accounts are subpoenaed, challenges and will likely lead to new precedent being established.

Circumstances may make a warrant unnecessary, such as when a social media profile is public (a public profile has no expectation of privacy, and to use it is thus not a search). If private electronic information (communication) is stored, the length of the storage matters under the federal Stored Communications Act- obtaining the content of communications stored less than 180 days requires a warrant. For information stored longer than that, a subpoena is likely sufficient. Emails and cloud data are the primary types of information you may want that would implicate the Stored Communications Act.

With a warrant, police have specific tools to retrieve electronic evidence from devices. This is known as forensic extraction; it can be done by copying or photographing files (manual extraction), or by software (logical extraction, where visible data is pulled from storage, or physical extraction, where the entire space of a device is accessible, including

deleted files). The scope of the warrant is extremely important when using this technology; use of a Cellebrite forensic extraction machine to obtain all the information off a device was upheld in *US v. Mann*, 592 F.3d 779 (7th Cir. 2009), where the actions taken during the search were within the scope of the warrant. However, use of similar software called Forensic Tool Kit was held to exceed the scope of a warrant in *U.S. v. Schlinghoff*, 901 F.Supp.2d 1101 (C.D. Ill. 2012), where officers used filters to find pornography in a warrant for immigration-related crimes. Although newer technology to obtain evidence is highly useful, traditional rules regarding search and seizure still apply and should be considered while conducting investigations.

See appendix for an example of a warrant affadavit for social media accounts.

Subpoena

Courts have held that there is no reasonable expectation of privacy in Internet Service Provider (ISP) subscriber information; thus, to obtain an IP address and account information, a subpoena to an ISP is sufficient. *Rader v.* State, 932 N.E.2d 755, 760 (Ind. Ct. App. 2010). This will be very useful in cases like possession of child pornography or solicitation where the downloading/ file sharing is probative of a crime.

Electronic Communications Privacy Act
[18 U.S.C. §§ 2510 et seq.; §§2701 et seq.; §§3121-27]

This federal law amended the federal Wiretap Act, discussed below, to include electronic communications. The Stored Communications Act mentioned above is Title II of the ECPA. Emails and other online messaging systems are within this law, and will likely require a warrant to access. Limited non-content information may be available through a subpoena. However, a normal subpoena may be insufficient; check the requirements of the ECPA, as an administrative subpoena (for subscriber information) may be needed. *In re Subpoena Duces Tecum to AOL,* 550 F. Supp. 2d 606, 611 (E.D. Va. 2008).

Draft emails are not considered communications under the ECPA, and thus can be obtained with a subpoena instead of a warrant (email drafts could be used to share information between different persons with access to an account, and could be highly relevant and probative of a crime).

State Law and Wiretapping

The State has tried to address electronic information issues, but the law is highly unsettled and constantly changing. Warrants for electronic information may be obtained currently, but the federal law should be complied with, as it is more settled.

Under IC 35-33.5-2-1, part of the Indiana Wiretap Act, only the state police department can install equipment to intercept electronic communication (this would be technology like a keystroke logger). This kind of equipment would be useful to obtain highly detailed information about a person's social media use, search history, and email records.

Consent:

Like other types of materials, electronic information may be obtained through a consensual search. The consent must be voluntary, not coerced. *See Doe v. Prosecutor, Marion County, Ind.*, 566 F. Supp. 2d 862 (S.D. Ind. 2008), where requirement for all sex offenders to provide warrantless searches of computers and devices at any time was held unconstitutional.

Preservation Letters

To prevent spoliation, whether intentional or inadvertent, preservation letters can help to ensure the availability of this evidence at trial and prove that the defendant was on notice of litigation so they had the opportunity to halt any document/ email destruction/ retention plan. A preservation letter can help get sanctions against a party if spoliation occurs. It is important to note that deleted documents are still recoverable through backup files on hard drives and servers, although the cost of obtaining the evidence may be excessive depending on available technology.

A preservation letter should clearly state the specific documents and information to be preserved, and the unique responsibilities of all affected persons based on their role in the litigation and their function within the company or place holding the evidence. The letter should:

• Describe the background of the case and how long it is expected to last;
• Identify information subject to preservation (paper and electronic);
• Specify pertinent data types and their associated applications, electronic and paper document preservation and retention methods, and preservation tools and how to use them;
• Inform employees of their legal obligations, including the ramifications and penalties for non-compliance with the litigation hold.

` *See generally, Samsung Electronics. Co., Ltd. v. Rambus, Inc.*, 439 F. Supp. 2d 524 (E.D. Va. 2006).

Finally, the letter should be reissued periodically to remind affected persons of their preservation obligations and duties. The preservation letter must be reissued if the issues or key players in the case change.

If you still fear spoliation, a temporary restraining order from a court, or in exceptional circumstances, an ex parte seizure order could be obtained. This would be useful to freeze or bar access to social media accounts, to prevent loss of evidence that could be extremely difficult or impossible to retrieve (given the many social media sites available, the nature of the information (rapidly changing and easily altered), and the ease of creating and deleting accounts, a protective order or seizure would likely be necessary, reasonable, and obtainable. A preservation letter will typically be sufficient for emails and is easy to use, but might not be practicable for social media accounts.

See appendix for sample preservation letters.

Problems:

Where a warrant or subpoena for an email account, computer data, or social media account is obtained, it is important to remember the vast nature of information contained in these sources. Where discovery is requested, it should be limited so compliance is not unduly burdensome or costly (which could result in a subpoena being quashed). However, discovery requests should be carefully considered, to include the variety of different devices which may play a role in crimes, from computers, to external hard drives, to third party possessors of information like OnStar vehicle safety systems, to MP3 players and USB drives. Consider what technologies could have been involved in the crime.

File formats are also an important consideration; although native file formats may be requested to obtain more accurate information, this may raise problems with metadata (making the request overbroad or overly invasive) and cost of converting file formats. *See Oki Am. v. Advanced Micro Devices*, No. 04-3171, 2006 WL 2547464 (N.D. Cal. Aug. 31, 2006). Courts are divided about whether or not metadata is discoverable, and more clear law may arise as technology, use, and understanding of technology develop.

CELL PHONES

What type of information?

Locational information, emails, web history, photos, call/ text records, contact lists, electronic transmissions

When is it useful?

Cell phone information can be used in a wide variety of cases, *if* the information can be obtained. Locational information is useful in nearly every type of case from murder and robbery (where access and timing/ opportunity are at issue) to juvenile offenses. Stored

call and text records, photos, and web history could be useful in most any case too. Although electronic communications like calls and emails could be useful, they may be difficult to get without a warrant because of federal law, as discussed above.

How to obtain:

Warrant:

Like emails, web history, and other computer-based forms of information, cell phone information is best obtained with a warrant. A warrant helps safeguard the evidence against later challenges. Additionally, cell phone information may implicate the Federal and Indiana Wiretap Acts such that a warrant or subpoena may be needed. The broad nature of cell phone information creates a reasonable expectation of privacy such that a search without a subpoena or warrant would most likely be unreasonable. Cell phones are different than the old land line phones discussed in *Smith v. Maryland* (the famous case holding that third party consent was sufficient to install a pen register, since call logs are "envelope" and not content information); cell phones contain a vast amount of different types of information. Even if the cell phone is unsecured by a password and the call log is easily accessible, this is a search and a warrantless search (even incident to arrest) is insufficient to protect individual privacy rights. *See Riley v. California*, 134 S.Ct. 2473, 2477 (2014). See below for a sample cell phone search warrant affadavit.

With a warrant, tracking information from the phone may also be used to locate a phone. The ECPA does not cover interception of device tracking signals. *See U.S. v. Bermudez*, 2006 WL 3197181 (S.D. Ind. June 30, 2006).

Subpoena

A subpoena to the phone company will be sufficient to access historical information (lists of numbers called and received, and the times of calls) under the ECPA. However, a subpoena will be insufficient for the actual content of calls, as there is a reasonable expectation of privacy in the content information. A warrant compliant with the ECPA or SCA, depending on the information sought, is needed to obtain this.

Search and seizure law regarding cell phones, like social media, is still developing as technology changes. This is another reason why subpoenas and warrants should be used to obtain evidence. *Riley* also addressed the lack of exigencies related to cell phones; if a phone is stored incident to arrest, it can be turned off, stored in a container to block signals, and the battery removed to prevent remote wiping. This allows time to obtain a warrant to search the stored information.

Cell phone locational information has been ruled to be akin to GPS, although there is ` disagreement over how much protection this information is entitled to. The constant and

extremely precise locational information gives an intrusive look into a person's movements and is thus subject to a reasonable expectation of privacy. *Com. v. Augustine*, 4 N.E.3d 846, 859 (Mass. 2014). The degree of privacy and the constancy of its monitoring overcomes the third party doctrine; as the Court in *Augustine* stated, cell phones are practically essential for social and business interaction. Although this case held that the privacy interest in cell phone locational data was so great that a warrant was required, other jurisdictions have disagreed. A subpoena could be sufficient in Indiana, but cases holding this have been cited negatively and could be overturned by new law. Thus, a warrant should be used even if it is not necessarily required.

Consent is a valid means of obtaining information from cell phones, just like other forms of evidence. **See appendix for a sample consent form.**

Wiretap Act [18 U.S.C. § 2510-2522]

The federal Wiretap Act protects oral, wire, and now electronic communications from interception without consent of at least one party to the communication. The law enforcement exception to consent allows officers to obtain a Wiretap Order from a federal judge to intercept communications. Providers of phone service also have a limited exception, and may intercept and monitor communications to prevent fraud and theft of service. The Wiretap Act and later amendments like the ECPA and SCA emphasize the importance of using valid warrants in obtaining communication information, whether electronic or telephonic.

Prosecutor Immunity

What is the doctrine of prosecutorial immunity?

Prosecutorial immunity is a common law doctrine insulating prosecutors from liability, so long as the prosecutor is acting within the proper authority and in a prosecutorial function. This doctrine is derived from sovereign and judicial immunity, the traditional idea that the government cannot be subject to liability without its consent. This immunity has been abrogated over the years, to now protect government acts within its official capacity.

Scope of immunity: absolute, qualified, or no immunity

Absolute- when a prosecutor is acting as an "officer of the court," doing acts intentionally associated with prosecution within the scope of legal authority, that prosecutor enjoys absolute immunity from §1983 suits. To determine whether activity is

prosecutorial, look at the nature of the function (whether governmental or administrative; see if the prosecutor is acting within the scope of employment as a prosecutor in a criminal case). *Fields v. Wharrie*, 740 F.3d 1107, 1110 (7th Cir. 2014) citing *Buckley v. Fitzsimmons*, 509 U.S. 59, 273-76 (1993).

Giving advice to police officers on an arrest warrant is prosecutorial and thus entitled to absolute immunity. *Spivey v. Robertson*, 197 F.3d 772 (5th Cir. 1999). Initiating prosecution, filing criminal charges, actions intimately associated with judicial proceedings, presenting the State's case, and evaluating evidence to decide whether to prosecute are all entitled to absolute immunity. Vouching for the truth of evidence is not, and thus, absolute immunity is lost. *Id.* at 776. Giving an officer legal advice during an investigation or doing the officer's investigation for him have also been held to not be a normal part of prosecution, and not entitled to absolute immunity.

Qualified immunity- for public officials performing discretionary functions. Qualified immunity is an affirmative defense; the burden rests on the defendant to raise it and establish the defense on a motion for summary judgment or at trial. *In re State Police Litigation*, 88 F.3d 111, 123 (2d Cir. 1996). Prosecutors performing non-prosecutorial functions and police officers generally are entitled to qualified immunity from civil liability so long as their actions could reasonably be thought consistent with the rights allegedly violated. *Anderson v. Creighton*, 483 U.S. 635, 638 (1987). Non-prosecutorial functions include administrative tasks like dealing with seized property and possibly investigating crimes generally (not in the course of putting together a specific case to prosecute).

No immunity- for municipalities in §1983 cases. No traditional immunity existed at common law for municipal corporations, and it was not the intent of Congress to limit municipality liability under §1983; for immunity to attach under this section, it must have been well-established under common law at the time §1983 was enacted. *Owen v. City of Independence*, 445 U.S. 622, 638 (1980). The Indiana Tort Claims Act (the State counterpart to §1983) may be found at IC 34-13-3-1 et seq. Prosecutors acting outside the scope of prosecutorial immunity may be subject to liability under these laws.

Problems:

Department policies- policy statements must be carefully drafted, as failure to comply with department policy has been used in federal equal protection lawsuits as evidence of discrimination. *See Soto v. Flores*, 103 F.3d 1056 (1st Cir. 1997). Policies should be carefully drafted to be fair and enforced equally to rebut claims of discrimination.

Ethical obligations/ professional responsibility: prosecutors must take care in the preparation, storage, and use of evidence to avoid acts that may lead to liability (e.g. for invasion of privacy or defamation). Although prosecutors may be entitled to absolute

immunity in prosecutorial functions, revealing or speaking about evidence or private facts outside of official duties would likely not be entitled to immunity. Other ethical rules like candor towards the tribunal and fairness to the opposing party are just as important; preparing evidence for trial is an important part of prosecutorial work, while falsifying and withholding evidence are sanctionable. It is important to remember that prosecutorial immunity is not completely absolute; this is why proper use of the investigatory tools discussed above matters.

Appendix

SUBPOENA DUCES TECUM

STATE OF INDIANA)
)
COUNTY OF RIPLEY)

IN THE RIPLEY CIRCUIT COURT

CAUSE NO.

IN THE MATTER OF AN
INVESTIGATION BY THE
BATESVILLE POLICE
DEPARTMENT
CASE # 1104256427

SUBPOENA DUCES TECUM

THE STATE OF INDIANA
RIPLEY COUNTY PROSECUTOR
VERSAILLES, IN 47042

TO: Cellco Partnership
DBA: Verzion Wireless
1-888-667-0028 (fax)

The keeper of the records of the **Cellco Partnership/Verizon Wireless** is hereby commanded to deliver to the Ripley County Prosecutor's Office, PO Box 102, 1158 N. Main Street,Versailles, IN 47042, **all subscriber information, including all calls, text messages made from April 25, 2015 to the present for the following number: xxx-xxx-xxxx**

Information is needed by the Ripley County Prosecutor's Office in regards to a pending criminal investigation being conducted now.

Date : May_____2015.

_____

Mary Ann McCoy

CLERK RIPLEY CIRCUIT COURT

RIPLEY COUNTY, INDIANA

RETURN

Came to hand _____, 2015, and is now returned served on the above named **Cellco Partnership**, ***via*** **fax # 888-667-0028** ***on this _____day of _____, 2015.***

_____

Signature

STATE OF INDIANA	)	IN THE RIPLEY SUPERIOR COURT
	) SS:	
COUNTY OF RIPLEY	)	CAUSE NUMBER:

IN THE MATTER OF AN
INVESTIGATION BY THE
RIPLEY COUNTY SHERIFF'S
DEPARTMENT

MOTION TO APPROVE PROSECUTOR'S SUBPOENA DUCES TECUM

Comes now the State of Indiana by its Prosecuting Attorney, Richard J. Hertel herein, and files Motion for Approval of Prosecutor's Subpoena Duces Tecum. Pursuant to *Oman v. State, 737 N.E.2d 1311 (Ind. 2000),* the State of Indiana is seeking leave of Court to issue the attached Subpoena Duces Tecum, the noted relevant records. Said Subpoena is relevant in purpose, sufficiently limited in scope, specific in directive so that compliance will not be unreasonably burdensome.

The State would respectfully request the issuance of said Subpoena Duces Tecum.

Respectfully submitted,

_____

Richard J. Hertel

Prosecuting Attorney

Eightieth Judicial Circuit

STATE OF INDIANA)
) SS:
COUNTY OF RIPLEY)

IN THE RIPLEY SUPERIOR COURT

CAUSE NUMBER:

IN THE MATTER OF AN
INVESTIGATION BY THE
RIPLEY COUNTY SHERIFF'S
DEPARTMENT

ORDER ON MOTION TO APPROVE PROSECUTOR'S SUBPOENA DUCES TECUM

Comes now the State of Indiana by Richard J. Hertel, Prosecuting Attorney for the Eightieth Judicial Circuit, having filed a written Motion to Approve Prosecutor's Subpoena Duces Tecum filed in the above referenced cause.

And the Court being duly advised now finds that said motion should be sustained.

IT IS THEREFORE ORDERED that the Motion to Approve Prosecutor's Subpoena Duces Tecum filed herein be, and the same is hereby sustained. Motion is granted.

_____ _____

DATE

Honorable Jeffrey Sharp

Ripley Superior Court

Cc: Prosecutor

SUBPOENA AD TESTIFICANDUM

May 20, 2015

Name

Address

Dear [Name],

You are being subpoenaed to testify in a juvenile trial as a result of the burglary of [place]. Your testimony is essential to establish that the burglary occurred and the damages resulted therefrom. Therefore, please be prepared to testify on that date to the information you supplied to the Prosecutor's office and/or police. In the event you have questions, please feel free to contact me.

Additionally, because trials often get continued, you may want to verify with my office that the trial is still scheduled the day before.

Sincerely,

Richard J. Hertel

Ripley County Prosecuting Attorney

SEARCH WARRANTS

A form for a sufficient search warrant affidavit is given in West's Annotated Indiana Code, In. St. 35-33-5-2:

STATE OF INDIANA)

) SS:

COUNTY OF _____)

A B swears (or affirms, as the case may be) that he believes and has good cause to believe (here set forth the facts and information constituting the probable cause) that (here describe the things to be searched for and the offense in relation thereto) are concealed in or about the (here describe the house or place) of C D, situated in the county of _____, in said state.

In accordance with Indiana Trial Rule 11, I affirm under the penalties for perjury that the foregoing representations are true.

_____

(Signed) Affiant Date

A search warrant form may be found in IC 35-33-5-3:

STATE OF INDIANA)
) SS:
COUNTY OF) IN THE _____ COURT

OF

To _____ (herein insert the name, department or classification of the law enforcement officer to whom it is addressed)
You are authorized and ordered, in the name of the State of Indiana, with the necessary and proper assistance to enter into or upon _____ (here describe the place to be searched), and there diligently search for _____ (here describe property which is the subject of the search). You are ordered to seize such property, or any part thereof, found on such search.
Dated this ____ day of _____, 20___, at the hour of ___ __M.

_____
(Signature of Judge)
Executed this ___ day of _____, 20___, at the hour of ____ ___M.

(Signature of Law Enforcement Officer)

INFORMATION SHARING AGREEMENT

STATE OF INDIANA)
) SS:
COUNTY OF RIPLEY)

IN THE RIPLEY CIRCUIT COURT

CAUSE NO. 69C01-0204-MI-

IN THE MATTER OF A COURT ORDER PERMITTING INTERAGENCY INFORMATION EXCHANGE

ORDER

Pursuant to Indiana Code 31-39-2-9 allowing and permitting interagency information exchange regarding juveniles under the jurisdiction of this Court and by the execution of an interagency agreement among the various local youth service providers, the Court recognizes the necessity and importance of sharing information regarding such youth as a significant means of providing not only a safer community, but also as a means of preventing delinquency.

It is therefore ordered by this Court that any information in the possession of the various youth providers, police departments, and school corporations concerning juveniles under the jurisdiction of this Court and their families, may be released to and exchanged among participants of such interagency agreement to further effectuate the purposes of that agreement (which agreement is attached hereto and made a part hereof and identified as Exhibit A) together with those other designated individuals representing such agencies and having a legitimate and official interest in such information as exchanged. This order in no way modifies the traditional roles of the Prosecutor, Probation Office and the Court in juvenile matters.

A release of any information to any person or agency other than those executing the referred to agreement shall remain subject to the statutes of the State of Indiana and rules of this Court.

SO ORDERED this _____ day of _____, 2002.

_____
Hon. Carl H. Taul
Judge of the Ripley Circuit Court

EXHIBIT A

COOPERATION AGREEMENT

This cooperation agreement is a systematic information based process designed to identify youth at risk and to provide appropriate services. This program emphasizes coordination and cooperation in the juvenile justice system (i.e. including schools and other community agencies) in the exchange of information as the foundation of effective prevention and intervention to reduce delinquent behavior.

We, the undersigned representing public and private agencies and institutions involved with the education, supervision and remediation of our community's children, do hereby enter into his agreement to develop and maintain a comprehensive community approach to the sharing of information. Such an approach will not only better enable us to serve children, but protect and enhance our community's well being.

In addition we further agree to specify personnel to serve as interagency contact persons as well as a representative to meet when necessary for the purpose to further these goals, and maintain the communications network, allowing for more effective prevention, intervention, and control services to be provided for the youth of our county.

Each Participating Agency Shall

Cooperate in the gathering of data for use by all participating agencies.

Make available to participating agencies data regarding delinquent acts and crimes that are allegedly committed.

Make available to participating agencies demographic information and incident information concerning juveniles within each agencies service.

Compile juvenile records in a useable format to be shared with participating agencies.

Develop a computer network, which is consistent with the goals of this agreement.

Maintain and respect the confidentiality of these exchanges of juvenile information. Safe guard the records of this system whether in electronic or written form.

This agreement does not authorize the release of information to any agency or person not party to this agreement, including but not limited to any news agency or other media, nor does it authorize the release of information regarding a juvenile that would otherwise violate Indiana law.

Those entering into this agreement are aware that their participation is to facilitate the exchange of information regarding juveniles and that the Prosecutor, Court and Probation Office have the final decision as to whether a formal delinquency petition should be filed or any court action taken.

MEDICAL RECORDS RELEASE

AUTHORIZATION FOR RELEASE OF MEDICAL INFORMATION

[Name of physician or other provider or institution]

Patient's Name: *[name of patient]*

Patient's Birthdate: *[date of birth of patient]*

Patient's Mailing Address: *[mailing address of patient]*

The undersigned authorizes:

[Name of provider or institution], *[address of provider or institution]*

To **release** the following portions of the **medical records** of the above named patient:

_____ Entire **medical record** for the period of *[begin date of period]* to *[end date]*

_____ The following specific portions of the **medical record**: *[description of portions]*

Release this information to: *[name of recipient]*

The **medical record** is needed for the following purpose: *[description of general purpose or intended use of **medical record**]*

I understand that I may revoke this **release** at any time, in writing, but the request shall remain valid until revoked or upon the expiration of *[number of days]* days, whichever occurs first, EXCEPT to the extent that action has been taken on such request. I also understand that this **release** may include **medical records** of treatment for physical and/or emotional illness, including treatment of alcohol or drug abuse. I also understand that HIV, AIDS, or AIDS-related information may be **released**. There is a potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected. Refusal to sign this authorization *[will/ will not]* result in the covered entity being unable to provide treatment, enrollment in the health plan, or eligibility for benefits.

Dated: *[date of execution]*

_____ *[Name of patient]*

Relationship (if other than patient): *[relationship to patient]*
In the presence of:
_____ *[Name of witness]*

Records Released by: *[name of releasor]*

Dated: *[date of **release**]*

SOCIAL MEDIA SEARCH WARRANTAFFIDAVIT

STATE OF INDIANA	)	IN THE RIPLEY SUPERIOR COURT
	)	
COUNTY OF RIPLEY	)	CAUSE NUMBER:

IN THE MATTER OF AN
INVESTIGATION BY THE
RIPLEY COUNTY SHERIFF'S
DEPARTMENT

AFFADAVIT OF PROBABLE CAUSE FOR SEARCH WARRANT

Comes now [name], and duly swears that he has Probable Cause to believe that evidence of a crime, to wit, **Failure to Register Required Information, Class D Felony; Synthetic Identity Deception, Class D Felony; Possession of Child Pornography, Class D Felony;** and/ or **Child Solicitation, Class D Felony** may be found in a Facebook account. The evidence to be searched for is as follows:

Any and all information for Facebook ID [URL] registered to [name] with the email address__; to include name and address; alternate email address; IP address and date and time of registration; account status; and log-in IP addresses associated with session times and dates.

The contents of any and all emails and instant messages stored in the above subscriber's Facebook account.

Any and all contents of electronic files stored in the subscriber's Neoprint, Photoprint, contact information, group contact information, and IP logs.

Any and all Facebook IDs listed on the subscriber's Friends List

Any and all methods of payment provided by the subscriber to Facebook

The basis for your affiant's belief that the above described evidence may be found in the above-mentioned devices is:

1. At all times herein your affiant was employed as [officer of x department]
2. On [date], your affiant was approached by A about strange behavior of D, which had been occurring on the public library's computer located in Osgood.
3. A was concerned because D is portraying himself as a young female named [x] during computer communications occurring at the library using a Yahoo! email account and Facebook account

4. A informed your affiant that she was aware of D's activities because it is her job to monitor content usage at the library. In essence, she could see what D was viewing as he viewed it. Based upon what she saw, she believed law enforcement should be involved.
5. A has provided your affiant with multiple screen captures. On these "screenshots" your affiant has observed folders memorializing D's communications with [young females]. Also, the females depicted on his Facebook account appear young.
6. In an effort to keep D's true identity concealed, his Yahoo! profile states that he will not use webcam, mic, or phone conversation.
7. Based upon training and experience, your affiant knows that individuals involved in child solicitation and/ or possession of child pornography often memorialize their communications with their victims and store child pornography for later viewing.
8. Your affiant investigated D's criminal history and found that he is a Registered Sex Offender for Possession of Child Pornography, Class D Felony, with a conviction date of __ in the Ripley Superior Court.
9. On [date], your affiant observed D's vehicle parked at the Osgood library. While dressed in plain clothes, your affiant entered the library and observed D sitting at a computer. Your affiant observed D's computer screen and saw D was logged into the Yahoo! account as __. He then opened the Facebook account. Your affiant took a photograph of D at the computer.
10. In paperwork completed by D and filed at the Ripley County Sheriff on [date] D stated he has "no" social networking information and provides an email account of [different email]. He made no reference to the accounts herein listed above. The paperwork states, *"Should any information change, I understand I have only 3 days to report such changes to the Ripley County Sheriff's Office."* Meyer has failed to report the Yahoo! and Facebook accounts.
11. Because D is a convicted se offender and has failed to provide the required account information and because D is fraudulently portraying his identity as a young female to young females, while memorializing the communications, based on your affiant's training and experience, your affiant believes and has probable cause to believe that the abovementioned requested information will prove that D did not provide the required registration information, that D used synthetic identifying information to profess to be a young female, as well as have a fair probability of containing evidence of additional criminal behavior, specifically possession of child pornography and/ or child solicitation.

Therefore, your affiant respectfully requests this Court to issue a Search Warrant based upon the above described information directing the search and seizure of the described items.

I swear under the penalty for perjury as specified by I.C. 35-44-2-1 that the foregoing representations are true.

Further affiant sayeth naught.

_____

Name

Department

PRESERVATION OF EVIDENCE LETTERS

Preservation Of Evidence Letter for Third Party

Dear _____,

Please be advised that [Prosecutor's Office] has reason to believe that electronic information in your company's control or possession may be relevant to the aforementioned legal matter.

Accordingly, discovery requests filed in this matter seek to collect and review electronic information within computer systems, removable electronic media, and other electronic devices owned and/or operated on behalf of [Company Name]. Sources of electronic information that must be preserved may include, but are not limited to, electronic documents, email and electronic correspondence, images and graphics, deleted files, spreadsheets, presentations, databases, system usage logs, Internet history and cache files, as well as enterprise user information, such as contact lists, calendars, task lists, etc.

Because electronic evidence can be both fragile and vulnerable to inadvertent destruction, [Affected party] has an obligation to take reasonable steps to ensure that electronic information is preserved until this matter has been resolved. Data preservation includes, but is not limited to, ceasing all data destruction activities, automatic email deletion functions, backup tape recycling, hard drive reformatting or defragmenting, and cache-clearing processes.

Laws and regulations barring the destruction of evidence directly apply to electronic evidence and any information created or stored in digital form that is relevant to a case. Failure to take all reasonable steps toward preserving electronic information may cause irreparable harm in this case and could result in sanctions against your [Company Name].

I would be happy to speak with you regarding this matter and provide further guidance or answer any questions.

Thank you for your attention to this matter.
Very truly yours,

_____

Preservation letter to defendant's counsel:

Preservation Of Evidence Letter

Dear: _____,

By this letter, you and your client[s] are hereby given notice not to destroy, conceal, or alter any paper or electronic files and other data generated by and/or stored on your client's [clients'] computers and storage media (e.g., hard disks, floppy disks, backup tapes), or any other electronic data, such as voicemail. As you know, your client's [clients'] failure to comply with this notice can result in severe sanctions being imposed by the Court {and liability in tort} for spoliation of evidence or potential evidence.

Through discovery we expect to obtain from you a number of documents and things, including files stored on your client's [clients'] computers and your client's [clients'] computer storage media. [As part of our initial discovery efforts, you {are hereby served with/will soon receive} {initial/supplemental} interrogatories and requests for documents and things.]

In order to avoid spoliation, you will need to provide the data requested on the original media. Do not reuse any media to provide this data.

Although [we may bring/have brought] a motion for an order preserving documents and things from destruction or alteration, your client's [clients'] obligation to preserve documents and things for discovery in this case arises in law and equity independently from any order on such motion.

Electronic documents and the storage media on which they reside contain relevant, discoverable information beyond that which may be found in printed documents. Therefore, even when a paper copy exists, we seek [will seek] all documents in their electronic form along with information about those documents contained on the media. We also seek [will seek] paper printouts of only those documents that contain unique information after they were printed out (such as paper documents containing handwriting, signatures, marginalia, drawings, annotations, highlighting, and redactions) along with any paper documents for which no corresponding electronic files exist.

Our discovery requests asks [will ask] for certain data on the hard disks, floppy disks, and backup media used in your client's [clients'] computers, some of which data are not readily available to an ordinary computer user, such as "deleted" files and "file fragments." As you may know, although a user may "erase" or "delete" a file, all that is really erased is a reference to that file in a table on the hard disk; unless overwritten with new data, a "deleted" file can be as intact on the disk as any "active" file you would see in a directory listing.

Courts have made it clear that all information available on electronic storage media is discoverable, whether readily readable ("active") or "deleted" but recoverable. See, e.g., Easley, McCaleb & Assocs., Inc. v. Perry, No. E-2663 (Ga. Super. Ct. July 13, 1994)("deleted" files on a party's computer hard drive held to be discoverable, and plaintiff's expert was allowed to retrieve all

recoverable files); Santiago v. Miles, 121 F.R.D. 636, 640 (W.D.N.Y. 1988)(a request for "raw information in computer banks" was proper and obtainable under the discovery rules); Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90, 112 (D. Colo. 1996)(mirror-image copy of everything on a hard drive "the method which would yield the most complete and accurate results," chastising a party's expert for failing to do so); and Northwest Airlines, Inc. v. Teamsters Local 2000, et al., 163 L.R.R.M. (BNA) 2460, (D. Minn. 2000)(court ordered image-copying by Northwest's expert of home computer hard drives of employees suspected of orchestrating an illegal "sick-out" on the Internet).

Accordingly, electronic data and storage media that may be subject to our discovery requests and that your client[s] are obligated to maintain and not alter or destroy, include but are not limited to those described below.

Introduction: Description Of Files And File Types Sought

All digital or analog electronic files, including "deleted" files and file fragments, stored in machine-readable format on magnetic, optical or other storage media, including the hard drives or floppy disks used by your client's [clients'] computers and their backup media (e.g., other hard drives, backup tapes, floppies, Jaz cartridges, CD-ROMs) or otherwise, whether such files have been reduced to paper printouts or not. More specifically, your client[s] is [are] to preserve all of your emails, both sent and received, whether internally or externally; all word-processed files, including drafts and revisions; all spreadsheets, including drafts and revisions; all databases; all CAD (computer-aided design) files, including drafts and revisions; all presentation data or slide shows produced by presentation software (such as Microsoft PowerPoint); all graphs, charts and other data produced by project management software (such as Microsoft Project); all data generated by calendaring, task management and personal information management ("PIM") software (such as Microsoft Outlook or Lotus Notes); all data created with the use of personal data assistants ("PDAs"), such as PalmPilot, HP Jornada, Cassiopeia, or other Windows CE-based or Pocket PC devices; all data created with the use of document management software; all data created with the use of paper and electronic mail logging and routing software; all Internet and Web browser-generated history files, caches and "cookies" files generated at the workstation of each employee and/or agent in your client's [clients'] employ and on any and all backup storage media; and any and all other files generated by users through the use of computers and/or telecommunications, including but not limited to voice mail. Further, you are to preserve any log or logs of network use by employees or otherwise, whether kept in paper or electronic form, and to preserve all copies of your backup tapes and the software necessary to reconstruct the data on those tapes, so that there can be made a complete, bit-by-bit "mirror" evidentiary image copy of the storage media of each and every personal computer (and/or workstation) and network server in your control and custody, as well as image copies of all hard drives retained by you and no longer in service, but in use at any time from [date] to the present.

Your client[s] is [are] also not to pack, compress, purge, or otherwise dispose of files and parts of files unless a true and correct copy of such files is made.

Your client[s] is [are] also to preserve and not destroy all passwords, decryption procedures (including, if necessary, the software to decrypt the files), network access codes, ID names, manuals, tutorials, written instructions, decompression or reconstruction software, and any and all other information and things necessary to access, view, and (if necessary) reconstruct the electronic data we [are requesting/will request] through discovery.

1. Business Records: [All documents and information about documents containing backup and/or archive policy and/or procedure, document retention policy, names of backup and/or archive software, names and addresses of any offsite storage provider.]

a. All email and information about email (including message contents, header information and logs of email system usage) {sent or received} by the following persons: [list names, job titles]

b. All other email and information about email (including message contents, header information and logs of email system usage) containing information about or related to: [insert detail]

c. All databases (including all records and fields and structural information in such databases), containing any reference to and/or information about or related to: [insert detail]

d. All logs of activity (both in paper and electronic formats) on computer systems and networks that have or may have been used to process or store electronic data containing information about or related to: [insert detail]

e. All word processing files, including prior drafts, “deleted” files and file fragments, containing information about or related to: [insert detail]

f. With regard to electronic data created by application programs which process financial, accounting and billing information, all electronic data files, including prior drafts, “deleted” files and file fragments, containing information about or related to: [insert detail]

g. All files, including prior drafts, “deleted” files and file fragments, containing information from electronic calendars and scheduling programs regarding or related to: [insert detail]

h. All electronic data files, including prior drafts, “deleted” files and file fragments about or related to: [insert detail]

2. Online Data Storage on Mainframes and Minicomputers: With regard to online storage and/or direct access storage devices attached to your client’s {clients’} mainframe computers and/or minicomputers: they are not to modify or delete any electronic data files, “deleted” files and file fragments existing at the time of this letter’s delivery, which meet the definitions set forth in this letter, unless a true and correct copy of each such electronic data file has been made and steps

have been taken to assure that such a copy will be preserved and accessible for purposes of this litigation.

3. Offline Data Storage, Backups and Archives, Floppy Diskettes, Tapes and Other Removable Electronic Media: With regard to all electronic media used for offline storage, including magnetic tapes and cartridges and other media that, at the time of this letter's delivery, contained any electronic data meeting the criteria listed in paragraph 1 above: Your client [clients] is [are] to stop any activity that may result in the loss of such electronic data, including rotation, destruction, overwriting and/or erasure of such media in whole or in part. This request is intended to cover all removable electronic media used for data storage in connection with their computer systems, including magnetic tapes and cartridges, magneto-optical disks, floppy diskettes and all other media, whether used with personal computers, minicomputers or mainframes or other computers, and whether containing backup and/or archive data sets and other electronic data, for all of their computer systems.

4. Replacement of Data Storage Devices: Your client [clients] is [are] not to dispose of any electronic data storage devices and/or media that may be replaced due to failure and/or upgrade and/or other reasons that may contain electronic data meeting the criteria listed in paragraph 1 above.

5. Fixed Drives on Stand-Alone Personal Computers and Network Workstations: With regard to electronic data meeting the criteria listed in paragraph 1 above, which existed on fixed drives attached to stand-alone microcomputers and/or network workstations at the time of this letter's delivery: Your client [clients] is [are] not to alter or erase such electronic data, and not to perform other procedures (such as data compression and disk de-fragmentation or optimization routines) that may impact such data, unless a true and correct copy has been made of such active files and of completely restored versions of such deleted electronic files and file fragments, copies have been made of all directory listings (including hidden files) for all directories and subdirectories containing such files, and arrangements have been made to preserve copies during the pendency of this litigation.

6. Programs and Utilities: Your client [clients] is [are] to preserve copies of all application programs and utilities, which may be used to process electronic data covered by this letter.

7. Log of System Modifications: Your client [clients] is [are] to maintain an activity log to document modifications made to any electronic data processing system that may affect the system's capability to process any electronic data meeting the criteria listed in paragraph 1 above, regardless of whether such modifications were made by employees, contractors, vendors and/or any other third parties.

8. Personal Computers Used by Your Employees and/or Their Secretaries and Assistants: The following steps should immediately be taken in regard to all personal computers used by your client's [clients'] employees and/or their secretaries and assistants.

a. As to fixed drives attached to such computers: (i) a true and correct copy is to be made of all electronic data on such fixed drives relating to this matter, including all active files and completely restored versions of all deleted electronic files and file fragments; (ii) full directory listings (including hidden files) for all directories and subdirectories (including hidden directories) on such fixed drives should be written; and (iii) such copies and listings are to be preserved until this matter reaches its final resolution.

b. All floppy diskettes, magnetic tapes and cartridges, and other media used in connection with such computers prior to the date of delivery of this letter containing any electronic data relating to this matter are to be collected and put into storage for the duration of this lawsuit.

9. Evidence Created Subsequent to This Letter: With regard to electronic data created subsequent to the date of delivery of this letter, relevant evidence is not be destroyed and your client [clients] is [are] to take whatever steps are appropriate to avoid destruction of evidence.

In order to assure that your and your client's [clients'] obligation to preserve documents and things will be met, please forward a copy of this letter to all persons and entities with custodial responsibility for the items referred to in this letter.

Sincerely,

_____

CELL PHONE SEARCH WARRANT AFFIDAVIT

STATE OF INDIANA, COUNTY OF FRANKLIN, SS:

PROBABLE CAUSE AFFIDAVIT FOR SEARCH WARRANT

Detective Michael A. Benjamin, of the Batesville Police Department, swears that he believes and has probable cause to believe that certain property, hereinafter described, is concealed in or upon the following described premises, to wit:

Cellco Partnership d/b/a Verizon Wireless

Custodian of Records

180 Washington Valley Road

Bedminster, NJ 07921

The evidence to be seized is described as follows:

Records maintained for the cellular telephone number of (xxx) xxx-xxxx from August 1st, 2014 to December 1st, 2015 regarding: Subscriber Information, call details, SMS or text messaging details and/or message content, call origination/termination location, cellular tower details, and/or GPS locations, voice mail content, all stored email, all web traffic, and/or all stored photographs

In Support of your affiant's assertion of Probable Cause, your affiant avers:

On [date] at approximately [time], the Batesville Police Department responded to the F Bank located at [address], Batesville, Franklin County, Indiana, for a report of a bank robbery.

Your affiant initiated an investigation and learned a white male entered the bank wearing [description]. The male was described by R, the bank teller who was robbed, as approximately _ tall and _ build. The male presented a note indicating he was robbing the bank and demanded money. Ms. R placed money into a white plastic bag with red lettering that the suspect provided her. He then left the bank on foot, ran in a northwestern direction, and was unable to be located. Your affiant also viewed bank surveillance footage of the suspect and confirmed the above information.

Your affiant learned from Dearborn County Detectives John Vance and Barry Bridges that on December 1st, 2010, the X Bank in Aurora, Indiana was robbed. This bank is located approximately 30 miles southeast of Batesville. The detectives told me, B (DOB:_) entered the X Bank in Aurora, Indiana and demanded money. After receiving the money he ran from the bank and was seen by witnesses getting into an older model [car] being driving by a male who they were able to identify as D (DOB☺. Both men were located and arrested by police a short time after the bank robbery. I was advised by investigating detectives that the money taken from the bank was recovered from the vehicle and was inside of a white plastic bag with red lettering. A

search warrant was obtained for the vehicle D was driving and a cell phone was located inside, which belonged to D.

On December 2nd, 2010, your affiant interviewed D concerning the F Bank Robbery in Batesville. D denied involvement and stated he at one time lived in the C Apartments in Batesville which was about 2 ½ to 3 years ago. He stated the last time he has been to Batesville was about a year and a half ago. C Apartments are located in a northwestern direction approximately ¾ of a mile from the F Bank. I also observed D's physical description of approximately _ tall and _ build to closely match the description of the same male who robbed the F Bank in Batesville.

On December 15th, 2010, your affiant met with D again. D confirmed (xxx) xxx-xxxx is his cell phone number. He also stated he has had it for about one or two years, his name is on the account, and the cell phone company is Verizon Wireless. I asked D if he would allow Verizon Wireless to release any and all cell phone records pertaining to his cell phone number xxx-xxx-xxxx, and he agreed. I read D his rights from a "consent to search" form and he signed the form. A copy of the signed consent form is attached to this search warrant affidavit.

As part of your affiant's training and experience, your affiant knows that computer, the internet, email, instant messaging, cellular telephones, and/or other electronic devices capable of two way communication have become part of the criminal enterprise.

Your affiant knows through training and experience that the service provider's for said communications devices maintain records in the normal course of business for subscriber information, transaction history, message content, call details, location of use, and other information that can be used in identifying the person using the device and/or the location of said use. As well as identifying additional persons involved in criminal activity.

Your affiant has identified the account records for telephone number (xxx) xxx-xxxx as being maintained by Cellco Partnership d/b/a Verizon Wireless.

Therefore, in order to further this investigation, your affiant respectfully requests the court to issue a search warrant directing the search for and seizure of the above described evidence.

I swear under penalty of perjury as specified by IC 35-44-2-1, that the foregoing representations are true.

_____

Detective Michael A. Benjamin

Probable cause found to issue search warrant.

_____

Judge, Franklin County Circuit Court

CELL PHONE CONSENSUAL RELEASE

CONSENT TO SEARCH CELLULAR TELEPHONE

Location: _____Date:____/____/_____Time _____:___m

Officer: _____Department: Batesville Police Department

Pursuant to *Pirtle v. State*, 323 N.E.2d 634 (Ind. 1975),
You have the following constitutional rights.
You have the right to require that a search warrant be obtained before any search of your property.
You have the right to refuse to consent of a warrantless search.
You have the right to talk to a lawyer before giving consent to such a search.
If you cannot afford a lawyer, one will be appointed for you.
If you are a juvenile, you have the right to talk with your parent or guardian before consenting to such a search.

WAIVER AND CONSENT

Both waivers and consents must be signed if juvenile.

I have read the statement of my rights and understand what my rights are.

I do not want a lawyer at this time. I consent to a warrantless search by officers of the Batesville Police Department of the following described cellular telephone:

MAKE:_____ MODEL:_____MOBILE #: _____

CARRIER:_____
PIN/PASSWORD_____

I authorize these officers to seize any items of data which they consider evidence. I understand and know what I am doing. No promises or threats have been made to me and no pressure or coercion of any kind has been used against me.

Signed_____

As a parent or legal guardian of
_____, I have read the juvenile's rights and my rights set out above and understand them. Neither the juvenile nor I want a lawyer at this time. The juvenile and I consent to the warrantless search of our property by officers of the Batesville Police Department. I authorize the officers to search the following described cellular telephone:

MAKE:_____ MODEL:_____MOBILE #: _____

CARRIER:_____
PIN/PASSWORD_____

I further authorize the officers to seize any items of data which they consider evidence. I understand and know what I am doing. No promises or threats have been made to me and no pressure or coercion of any kind has been used against me.

Signed_____

Witness:_____

Witness:_____

Date:_____/_____/_____Time:_____:____m